PassQueen
a.k.a dumpsqueen.com

CyberArk CDE-CPC Recertification

CyberArk CPC-CDE-RECERT

Version Demo

Total Demo Questions: 12

Total Premium Questions: 122

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

What is the correct CyberArk user to use when installing the Privilege Cloud Connector software?

A. installeruser@

B. Administrator

C. _admin

D. Installer

ANSWER: A

Explanation:

installeruser@<suffix> is the dedicated CyberArk account used to install and register the Privilege Cloud Connector. CyberArk provides this installer identity as part of the Privilege Cloud tenant onboarding and setup process. The <*suffix*> represents the tenant-specific portion supplied by CyberArk, so the installer must use the complete account name exactly as provided for that tenant. This account is intended for the connector-installation workflow and enables the installation package to authenticate to the Privilege Cloud service, securely register the connector, and obtain the configuration required for it to communicate with the tenant.

Using the designated installer identity also supports CyberArk's separation of duties: installation and connector registration are performed with a purpose-built account rather than a general administrative identity. Before beginning the installation, confirm that the installer has the tenant-specific username and the associated credentials supplied in the Privilege Cloud welcome or onboarding materials. Follow the connector installation steps and prerequisites in the CyberArk Privilege Cloud documentation: Install the Privilege Cloud Connector and CyberArk Documentation.

QUESTION NO: 2

After the session has ended, where is the default final recording storage located?

A. CyberArk Privilege Cloud

B. Privilege Cloud Connector

C. Network attached storage

D. User workstation

ANSWER: A

Explanation:

The correct answer is **CyberArk Privilege Cloud**. Privileged Session Manager recordings are created locally on the Privilege Cloud Connector only while a session is in progress, ensuring that the connector can capture session activity. After the session ends, the recording is uploaded to the Privilege Cloud Vault for durable, centralized storage. By default, these completed session recordings are stored in the **PSMRecordings** Safe. This central Vault storage allows authorized users to locate, play back, audit, and retain recordings under the organization's CyberArk access controls and retention practices. Storing completed recordings in Privilege Cloud also supports centralized monitoring and investigation workflows rather than leaving the final copy on the connector that brokered the connection. CyberArk documentation describes how PSM records privileged sessions and stores the recordings in the Vault, while Privilege Cloud documentation identifies the connector's role in brokering and recording sessions before the resulting data is managed by the Privilege Cloud service. See CyberArk: Privileged Session Manager overview and CyberArk: Privilege Cloud Connectors.

QUESTION NO: 3

Which statement is correct about using the AllowedSafes platform parameter?

A. It allows users to access accounts in specific safes.

B. It prevents the CPM from scanning all safes, restricting it to scan only safes that match the AllowedSafes configuration.

C. It allows the CPM to access PSM safes to monitor platform configuration and connection component changes.

D. It prevents the CPM from processing pending items in the Discovery safes enforcing manual intervention to complete the onboarding process.

ANSWER: B

Explanation:

The correct statement is: “It prevents the CPM from scanning all safes, restricting it to scan only safes that match the AllowedSafes configuration.” The `AllowedSafes` platform parameter controls the scope of Safes that the Central Policy Manager (CPM) evaluates for accounts assigned to that platform. Rather than searching every Safe to locate accounts requiring password-management activity, the CPM uses the configured Safe names or matching pattern to limit its search to the intended Safes. This is particularly useful in large environments, where platforms may be dedicated to particular business units, environments, account populations, or operational teams. Limiting the Safe scope improves efficiency by reducing unnecessary scanning and helps implement a cleaner operational boundary for a platform’s password-management workload. The parameter therefore affects CPM account discovery and processing scope for that platform; it is not a user authorization setting. Configure the value carefully so that every Safe containing accounts assigned to the platform is included or matched; accounts outside the configured scope will not be picked up by CPM processing for that platform. CyberArk platform configuration guidance is available in the CyberArk PAM Self-Hosted platform documentation and the CyberArk Privilege Cloud platform documentation.

QUESTION NO: 4

A security review is performed immediately after a successful PSM for SSH installation. The reviewer wants to remove temporary installation artifacts that contain sensitive setup information and are no longer required for normal operation. Which files should be deleted? (Choose two.)

A. Delete the `user.cred` file used during installation.

B. Delete the `vault.ini` file used during installation.

C. Delete the `psmpparms` file used during installation.

D. Delete the PSM for SSH service configuration files.

ANSWER: A B

Explanation:

The `user.cred` file used during installation should be deleted because it contains credential material used by the installer to authenticate to the Vault. Retaining this temporary credential artifact unnecessarily increases local exposure.

The installation copy of `vault.ini` should also be deleted after successful installation because it contains Vault connectivity information used during setup. The `psmpparms` configuration file is not identified as a temporary credential artifact that must be removed as part of this post-installation cleanup.

QUESTION NO: 5

Which method can be used to directly authenticate users to PSM for SSH? (Choose three.)

A. CyberArk authentication

B. LDAP authentication

C. RADIUS authentication

D. Windows authentication

E. SAML authentication

F. OpenID Connect (OIDC) authentication

ANSWER: A B C

Explanation:

PSM for SSH supports direct user authentication to the CyberArk Vault before the user opens an SSH-based privileged session. The supported methods in this authentication flow are CyberArk authentication, LDAP authentication, and RADIUS authentication. CyberArk authentication validates the user against a CyberArk Vault user account and its Vault credentials. LDAP authentication enables users who are defined through the configured LDAP integration to authenticate with their directory credentials, allowing centralized enterprise identity management. RADIUS authentication enables authentication through the organization's RADIUS server and can support challenge-response flows, which are commonly used with multi-factor authentication mechanisms. After successful authentication, PSM for SSH applies the user's Vault permissions and Safe access rights to determine which privileged accounts and connection actions are available. These methods are specifically configured for the PSM for SSH authentication process and allow access to be evaluated by the Vault before session establishment. CyberArk's PSM for SSH documentation describes configuring user authentication methods, including CyberArk, LDAP, and RADIUS authentication. See the CyberArk PSM for SSH documentation and the CyberArk LDAP integration documentation.

QUESTION NO: 6

Which ports do the CyberArk Identity Connector require to be opened to support using Active Directory for LDAP authentication to Privileged Cloud Shared Services? (Choose two.)

A. TCP 636 from the connector host to the domain controller

B. TCP 443 from the connector host to the CyberArk Tenant

C. TCP 636 from the CyberArk Tenant to the domain controller

D. TCP 443 from the CyberArk Tenant to the connector host

E. TCP 636 from the domain controller to the CyberArk Tenant

ANSWER: A B

Explanation:

TCP 636 from the connector host to the domain controller is required when Active Directory authentication is configured through secure LDAP (LDAPS). The Identity Connector acts as the component within the customer network that queries Active Directory. Therefore, it must be able to initiate a secure LDAP connection to a domain controller on TCP 636. This permits the connector to validate credentials and retrieve the directory information needed for authentication without exposing the domain controller directly to the CyberArk Identity service.

TCP 443 from the connector host to the CyberArk Tenant is also required because the connector establishes outbound HTTPS communication with the CyberArk Identity tenant. This outbound communication model allows the tenant to use the connector for access to on-premises directory services while avoiding a requirement for inbound connectivity from the internet into the customer environment. The connector must be able to reach the tenant over HTTPS so that authentication-related requests and connector service communications can be securely exchanged. CyberArk documentation describes the Identity Connector as requiring outbound internet connectivity, including HTTPS, and documents its role in connecting CyberArk Identity to on-premises directories. See CyberArk Identity Connector installation documentation and CyberArk Identity LDAP directory documentation.

QUESTION NO: 7

During CPM hardening, which locally created users are granted Logon as a Service rights in the local group policy? (Choose 2.)

A. PasswordManager

B. PluginManagerUser

C. ScannerUser

D. PasswordManagerUser

E. CPMServiceAccount

ANSWER: C D

Explanation:

During CPM hardening, the hardening procedure configures the Windows local security policy so that **ScannerUser** and **PasswordManagerUser** have the *Log on as a service* user right. These are locally created CPM-related identities whose assigned service-logon capability allows the applicable CPM components to start and run under their designated restricted accounts rather than relying on an interactive administrator account. Granting this right is a required part of the hardening configuration because Windows checks the local or domain user-rights assignment when a service attempts to start with a particular account. The hardening process applies this assignment through the Local Group Policy security settings, alongside other security restrictions intended to reduce the CPM server's attack surface. CyberArk documents this action explicitly in the CPM hardening task description under the step that adds users to Local Group Policy Security settings. Use the documented hardening workflow and verify the resulting assignment in the server's Local Security Policy after implementation, particularly where domain Group Policy might later overwrite local user-rights assignments. See CyberArk's CPM hardening task descriptions and its CPM server hardening guidance.

QUESTION NO: 8

Which Safe(s) does the AllowedSafes=Win platform parameter configuration match? (Choose two.)

A. WindowsPasswords

B. win-ssh-keys

C. CXD-WIN-ADMINS

D. SQL-Win-SA

E. WiNdOwS_Accts

ANSWER: A D

Explanation:

`AllowedSafes=Win` matches `WindowsPasswords` and `SQL-Win-SA`. In CyberArk platform configuration, the AllowedSafes setting controls the Safes in which a platform may be used, and its value is evaluated as a regular expression. Because the expression is simply `Win`, without beginning or ending anchors, it matches a Safe name wherever that exact character sequence occurs within the name. `WindowsPasswords` contains the exact substring `Win` at its beginning, while `SQL-Win-SA` contains the same exact substring in the middle of the Safe name. Regular-expression matching for this parameter is case-sensitive, so the capitalization in the configured expression must match the Safe name exactly. The relevant match is therefore the capital `W` followed by lowercase `in`. This configuration is useful when an administrator wants to permit a platform in multiple Safes whose names share a consistent naming component, without listing every Safe individually. For more information about configuring platform properties and Safe restrictions, see CyberArk's platform configuration documentation and the platform properties reference.

QUESTION NO: 9

What is the default username for the PSM for SSH maintenance user?

A. proxymng

B. psmp_maintenance

C. *psmpmaintenanceuser*

D. proxyusr

ANSWER: A

Explanation:

`proxymng` is the default local maintenance-user account created for PSM for SSH. This account is intended for administrative and maintenance activities required by the PSM for SSH infrastructure, rather than for normal privileged-session access. During installation and configuration, CyberArk uses distinct operating-system accounts for PSM for SSH components and operational purposes; knowing the maintenance account name is important when following installation, hardening, troubleshooting, or service-management procedures. Administrators should retain the account unless a documented CyberArk procedure specifically instructs otherwise, and they should protect it according to organizational Linux-account and privileged-access controls. In particular, changes to its permissions, ownership, shell configuration, or related service dependencies should be made only with an understanding of the PSM for SSH deployment requirements, because these settings can affect the component's ability to operate and be maintained. CyberArk's PSM for SSH documentation is available in the CyberArk Documentation portal; consult the version-specific installation and maintenance guidance for the deployed PAM Self-Hosted release. CyberArk's Privileged Session Manager overview also provides product context for the session-management capabilities supported by the platform.

QUESTION NO: 10

Your customer recently merged with a smaller organization. The customer's connector has no network connectivity to the smaller organization's infrastructure. You need to map LDAP users from both your customer and the smaller organization. How is this achieved?

A. Create the required users in one directory and configure the Identity Connector to read that directory, as there can only be one Identity Connector.

B. Create mappings for both directories from the original Identity Connector.

C. Deploy Identity Connectors in the newly acquired infrastructure and create user mappings.

D. Switch all users to SAML authentication as there can only be one Identity Connector.

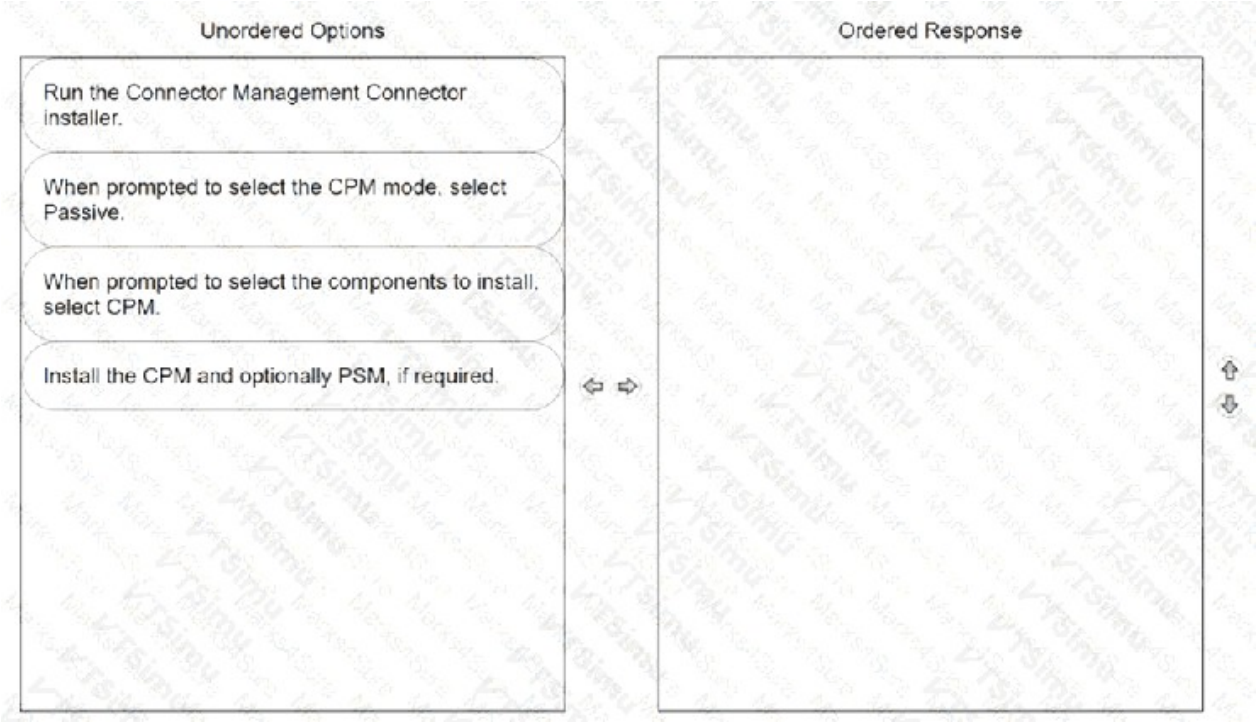
ANSWER: C

Explanation:

Deploy Identity Connectors in the newly acquired infrastructure and create user mappings. An Identity Connector must be able to communicate with the LDAP directory that is the source of the users being mapped. Since the existing connector has no network route to the acquired organization's infrastructure, it cannot query or authenticate against that organization's LDAP directory. Installing an additional Identity Connector within the acquired organization's reachable network establishes the required local connectivity to its directory without requiring a network connection from the original connector. The additional connector can then be registered with the same Privilege Cloud tenant and used when configuring an LDAP user mapping for that directory. The existing connector continues to service mappings for the customer's original directory, allowing both independent directory environments to provide users to the same Privilege Cloud deployment. This distributed connector design is particularly appropriate after mergers, when directory services and network boundaries commonly remain separate. CyberArk documents Identity Connectors as the component that connects Privilege Cloud to enterprise directories and supports directory-based user management. See the CyberArk Identity Connector documentation and the Privilege Cloud user management documentation.

QUESTION NO: 11 - (SIMULATION)

Arrange the steps to install passive CPM using Connector Management in the correct sequence



ANSWER: Check the explanation for the answer

Explanation:

The correct sequence to install a passive CPM through Connector Management is:

This order starts the Connector Management installation workflow, launches the CPM/optional PSM installation, selects CPM as the installed component, and then configures that CPM instance as passive.

QUESTION NO: 12

Which tool configures the user object that will be used during the installation of the PSM for SSH component?

A. CreateUserPass

B. CreateCredFile

C. ConfigureCredFile

D. ConfigureUserPass

ANSWER: B

Explanation:

CreateCredFile is the utility used to configure the credentials associated with the Vault user object required by PSM for SSH. During deployment, PSM for SSH needs a securely stored set of credentials so it can authenticate to the CyberArk Vault and perform its required component operations. CreateCredFile creates the protected credential file containing the relevant Vault-user authentication data, rather than leaving those credentials exposed in plain-text configuration files or requiring interactive entry whenever the service is used. This credential-file creation step is therefore part of preparing the PSM for SSH installation and its Vault connectivity. The user object must already have the appropriate authorizations and be associated with the expected PSM for SSH configuration; CreateCredFile then establishes the secure local credential material that the component uses. For CyberArk product documentation and current installation guidance, consult the CyberArk Documentation portal and the CyberArk Privileged Access Manager product resources.